

CLAIM AMENDMENTS

1. (PREVIOUSLY SUBMITTED) A method for secured access to data in a network including an information center and a plurality of data area access systems in which permission to store said data and to define, at the information center, access rights of third parties to said data is limited to the owner of rights to said data, said method comprising the steps of:

a) in each case storing the data only once in one of said data area access systems not accessible to the owner of the rights; then

b) registering the presence of data of a certain type in each data area access system at said information center, followed by the owner of the rights to the stored data, should he wish, defining access rights of third parties to said data at said information center;

c) transmitting a list of the data present of a certain type, specifying the data area access system storing said data, from said information center to a requesting data area access system for which the access rights of said requesting data area access system correspond to the access rights defined at said information center for said data, and after a request of a requesting data area access system for data of said certain type; and then

d) directly transmitting said data of said certain type

by said data area access system storing said data to said requesting data area access system subject to said data area access system storing said data having received a confirmation from said information center.

2. (ORIGINAL) A method as defined in Claim 1 wherein
an authorization of the storage of data and of the definition of
the access rights of third parties to the data takes place by
means of an identity check of the owner of the rights to the
data.

3. (ORIGINAL) A method as defined in Claim 1 or 2,
wherein data to be stored are stored in said data area access
system with an electronic form which contains the type of the
data.

4. (ORIGINAL) A method as defined Claim 1 wherein a data area access system (1) storing data responds to a request for certain data of a certain type by a requesting data area access system (2) by verifying the access rights through an inquiry to the information center (3) as to whether the requesting data area access system has access rights to the certain data of a certain type.

5. (ORIGINAL) A method as defined in Claim 1, wherein
a data area access system receiving certain data of a certain
type allows access to the received data only directly after a
respective reception of said data.

6. (ORIGINAL) A method as defined in Claim 1, wherein
a data area access system storing certain data of a certain type
grants access to the certain data of a certain type only if a
positive verification has taken place through an inquiry to the
information center as to whether said data area access system
storing said certain data of a certain type can show access
rights for said certain data of a certain type.

7. (ORIGINAL) A method as defined in Claims 1 wherein the information center is notified by a data area access system having new data about the presence of new data of a certain type, whereupon said information center sends a notifying confirmation to the data area access system.

8. (ORIGINAL) A method as defined in Claim 1 wherein said data are identified on the basis of an identification which is allocated as a unique identification by said information center and is transmitted by said information center after a registration of new data to the data area access system storing said data, in order for said system to append the respective identification to the respective data.

9. (ORIGINAL) A method as defined in Claims 1 wherein, after an inquiry for data of a certain type by a data area access system, said information center prepares a list of all the data present of this certain type before it verifies the access rights to the data of the certain type, in order to transmit the list of data present of this certain type, specifying the data area access system respectively storing these data, to the requesting data area access system for which the requesting data area access system can show said access rights.

10. (ORIGINAL) A method as defined in Claim 1 wherein, when data access is desired by a data area access system to data of a certain type, firstly a request for such data of the certain type is sent to the information center.

11. (ORIGINAL) A method as defined Claim 1 wherein, when data transmission is desired from a data area access system storing data to a requesting data area access system, firstly a request for certain data of a certain type is sent by the latter system to the data area access system storing these certain data of a certain type.

12. (ORIGINAL) A method as defined in Claim 1, wherein the data in a data area access system are stored in a secure data memory, no direct access being possible to the data stored therein.

13. (ORIGINAL) A method as defined in Claim 1 wherein the type of the data is determined by their content and/or the owner of the rights to the data.

14. (ORIGINAL) A method as defined in Claim 1 wherein the access rights to stored data can be defined by the owner of the rights to the data at any point in time after their registration at the information center and, after that, can be changed again as desired by a re-definition by the owner of the rights to the data.

15. (ORIGINAL) A method as defined in Claim 1 wherein the access rights to stored data can be granted by the owner of the rights to the data when they are stored in a data area access system.

16. (ORIGINAL) A method as defined in Claim 1 wherein communication between a data area access system and the information center or another data area access system takes place in encrypted form.

17. (ORIGINAL) A method as defined in Claim 16,
wherein the sender provides the information sent by him with a
digital signature by means of a secret signature code, whereby
the recipient can verify the sent information by means of an
associated public signature code.

18. (ORIGINAL) A method as defined in Claim 16 or 17 wherein the sender encodes all transmitted data by means of a public encryption code issued by the recipient, whereby only the recipient can decode the transmitted data by means of a secret encryption code.

19. (ORIGINAL) A method as defined in Claim 16 wherein not only each data area access system and the information center but also each participant has a secret signature code and a secret encryption code and a public signature code and a public encryption code.

20. (ORIGINAL) A method as defined in Claim 19 wherein the secret signature codes and encryption codes and/or public signature codes and encryption codes of a participant are stored on a data carrier, such as a smart card.

21. (ORIGINAL) A method as defined in Claim 1 wherein a participant accessing the network must authorize himself and his identity is verified by the information center.

22. (ORIGINAL) A method as defined in Claim 21
wherein the identity of a participant is stored on a data carrier
such as a smart card.

23. (ORIGINAL) A method as defined in Claim 1 wherein the permission for storing the data is given by the owner of the rights to the data at the latest when the data are registered at the information center, said information center not allowing any subsequent data access to these data without correct authorization.

24. (ORIGINAL) A method as defined in Claim 1 wherein, when the data are transmitted, the appropriation specified by the owner of the access rights for the transmission of these data in the original data context is transmitted together with these data in the form of an electronic watermark and these data are additionally marked visibly as an appropriated copy of the original data.

25. (NEW) A system comprising:

a) a plurality of data area access systems, each having a secure data memory associated therewith; and

b) an information center, wherein (I) said system is configured and adapted such that entry of a piece of data into said system comprises a writing of said piece of data to a respective one of said secure data memories that can only be effected by an authorized user of the data area access system associated with the respective secure data memory and in conjunction with the authorization of an authorized user of said information center, (ii) said information center is configured and adapted for storing information that defines respective access rights for each piece of data entered into the system, (iii) said system is configured and adapted such that display and modification of the information defining the access rights to said entered piece of data is restricted to said authorized user of said information center, in conjunction with whose authorization said entry was effected, and (iv) said system is configured and adapted such that access to any piece of data entered into the system is restricted to those authorized users of the system having appropriate access rights as defined by said information for the piece of data to be accessed.

26. (NEW) The system of Claim 25, wherein said system is configured and adapted such that access to any piece of data entered into the system can be effected solely via the data area access systems and solely by authorized users of the respective data area access system via which access is to be effected.

27. (NEW) The system of Claim 26, wherein all authorized users of said information center are not authorized to use any of said data area access systems.

28. (NEW) The system of Claim 25, wherein one or more of said data area access systems are operable in a mode in which an authorized user of said information center who is not an authorized user of the respective data area access system.

a) can display and modify that part of said information defining access rights that is not restricted from display and modification by them,

b) yet cannot access any pieces of data entered into the system.

29. (NEW) The system of Claim 26, wherein said mode allows an authorized user of said information center who is not an authorized user of the respective data area access system to retrieve a list of pieces of data that were entered into the system in conjunction with their authorization.

30. (NEW) The system of Claim 25, wherein use of each of said data area access systems is restricted to a respective set of authorized users.

31. (NEW) The system of Claim 25, wherein said system is configured and adapted for effecting communication between any of said information center and said data area access systems in an exclusively secure manner.

32. (NEW) The system of Claim 25, wherein said system is configured and adapted such that exclusively said secure data memories serve to store any pieces of data entered into said system.

33. (NEW) The system of Claim 25, wherein said system is configured and adapted for confirm both user authorization and the authorized user's access rights each time a piece of data entered into the system is to be accessed.

34. (NEW) The system of Claim 25, wherein

- a) said system is configured and adapted for deriving information from pieces of data entered into said system, and
- b) access to any part of said derived information is restricted to the same extent as the pieces of data form which it is respectively derived.

35. (NEW) The system of Claim 25, wherein

a) said system is configured and adapted for complementing pieces of data entered into said system with referenced information, and

b) access to any part of said reference information is restricted to the same extent as the pieces of data it respectively complements.

36. (NEW) The system of Claim 25, wherein said system is configured and adapted for insuring that pieces of data entered into said system are not replicated within the system.